УДК
004.056.57

Журавльов А.М

Дослідження моделей розподілення ресурсів для забезпечення доступності в системах безпеки

Вінницький національний технічний університет

Анотація

Дана робота присвячена вивченню та аналізу існуючих моделей розподілення ресурсів для забезпечення доступності в системах безпеки. Новизна даної роботи полягає в детальному дослідженні існуючих систем розподілення ресурсів і аналіз їх ефективності в різних моделях забезпечення інформаційної безпеки.

Ключові слова: моделі розподілення ресурсів, доступність системи, модель Мілена, засоби масової інформації, безпека інформаційних і комунікаційних систем.

Abstract

This paper is devoted to the study and analysis of existing resource allocation models to ensure availability in security systems. The novelty of this work consists in a detailed study of existing resource allocation systems and an analysis of their effectiveness in different models of information security.

Keywords:
resource allocation model, system availability, Milena's model, media, information and communication security systems.

Вступ

Розвиток сучасних інформаційних і комунікаційних технологій впливає на усі сфери людської життєдіяльності, підвищуючи їх ефективність і, одночасно, породжуючи множину не контрольованих загроз. На сьогодні головними і найбільш визначальними міжнародними стандарти в сфері інформаційної безпеки є стандарти серії ISO 27000. Саме на них базуються системи розподілення ресусів.

У даній роботі буде проведений аналіз систем розподілення ресурсів зокрема моделі розподілення ресурсів на основі моделі Мілена. Проведено її ретельний аналіз і визначення усіх її переваг і недоліків в порівнянні з іншими системами.

Основна частина

У роботі розглянуті проблеми як виникають в системах розподілення ресурсів їх основні характеристики. Поставлено задачу аналізу переваг та недоліків досліджених методів.

Було виявлено, що теоретичне підгрунтя для створення сучасних СПЗ виступають політика безпеки й моделі безпеки, які відображають процеси НСД на інформацію та регулюють механізми її захисту. Під політикою безпеки розуміють інтегральну і, як правило, якісну характеристику, що описує властивості, принципи та правила захищеності інформації в ІМД в загальному просторі загроз. Модель безпеки являє собою формалізоване (математичне, аморетмічне, схемотехнічне тощо) подання обраної політики безпеки. Головним призначенням моделей безпеки є вибір та обґрунтування базисних принципів архітектури, що визначають механізми реалізації засобів захисту інформації, підтвердження властивостей (наприклад, рівня захищеності інформації) системи, яка розробляється шляхом формального доведення дотримання політики безпеки, складання формальної специфікації політики безпеки новостворювальної СПЗ, тощо

Детально проаналізувавши лише ті стохастичні та динамічні моделі, які отримані найбільше розповсюдження.

Було вибрано модель захисту від загроз відмов в обслуговуванні (модель Мілена) як одну з найбільш головних і досконалих моделей за допомогою реалізації якої можна побудувати систему забезпечення доступності.

Результати та висновки

Дана модель була проаналізована і було визначено як повинен бети реалізований процес створення системи розподілення ресурсів щоб домогтись найбільшої захищеності.Проте реалізація цієї моделі з іншими сучасними напрацюваннями в галузі інформаційної безпеки може принести кращі результати..

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Tutorial on Principal Component Analysis [Електронний ресурс] // Center for Neural Science, New York University. – 2009. – Режим доступу до ресурсу: http://ic.unicamp.br/~rocha/teaching/2011s2/mc906/aulas/pca-tutorial-01.pdf.
2. Christodorescu M. Mining Specifications of Malicious Behavior [Електронний ресурс] /M. Christodorescu, S. Jha, C. Kruegel. – 2007. – Режим доступу до ресурсу:

https://pdfs.semanticscholar.org/f1de/136249e1322bb95bc17611a844d207ad93a8.pdf
3. Sai S. Signature Generation and Detection of Malware Families [Електронний ресурс] / S.Sai, K. Pankaj, B. Bezawada // Centre for Security, Theory and Algorithmic Research (C-STAR) International Institute of Information Technology Hyderabad - 500032, India. – 2008. – Режим доступу до ресурсу: https://vxheaven.org/lib/pdf/Signature%20Generation%20and%20Detection%20of%20Malware%20Families.pdf
4. Новіков О. М. Безпека Інформаційно-Комунікаційних Систем / О. М. Новіков, М. В. Грайворонський. – Київ: BHV, 2009. – 608 с. – (Підручник).
5. Лігачова Н. Маніпуляції на ТБ. Маніпулятивні технології в інформаційно-аналітичних телепрограмах українського телебачення: моніторинг, рекомендації щодо захисту від впливу та запобігання застосуванню. Принципи відкритої редакційної політики телеканалів / Н. Лігачова, С. Черненко, В. Іванов. Київ : Телекритика, Інтерньюз-Україна – 2003.

Журавльов Андрій Михайлович– студент групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: a.zhuravlov1997@gmail.com

Науковий керівник: ***Поплавський Анатолій Вацлавович*** - кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Zhuravlov Andrii Mihailovich - student of UB-14b group, faculty of management and information security, Vinnytsia national technical university, Vinnytsia, e-mail: a.zhuravlov1997@gmail.com

Supervisor: ***Poplavskii Anatolii Vatslavovich*** - candidate of technichal Sciences, associate Professor of management and security of information systems, Vinnytsia national technical University, Vinnytsia.